International Journal of Recent Advances in Information Technology & Management
Vol. 2, Issue 2 - 2018

A NOVEL HYBRID SWITCHING FRACTIONAL ORDER ENCRYPTION ALGORITHM USING CHAOTIC SYSTEMS

ANUJESUS DHARMARAJ[*], IGNATIUS A HERMAN[**]

ABSTRACT

The hazardous development of PC and system innovation, the issue of security in picture data transmission and capacity draws more attention. Image encryption has turned into a vital point in the field of systems administration and communications. Image encryption is not quite the same as content encryption and more entangled because of some inside highlights like clamorous properties like boundedness, intrinsic arbitrariness. A few methodologies on turbulent frameworks for picture encryption has been proposed .Yet a large number of them center around the fragmentary request clamorous frameworks and secure communication. In this paper, another exchanging partial request confused framework is presented which contains partial request chen frameworks and other two partial request disordered frameworks. The proposed strategy utilizes the exchanging fragmentary request disorderly frameworks to picture encryption utilizing restrictive or (XOR) encryption algorithm. The encryption plan could expand irregularity and enhance speed of encryption. The encryption calculation has three process in particular the stage process, the dissemination process and the blending RGB Channels process, The proposed novel cross breed exchanging fragmentary request encryption calculation strategy has a significantly predominant encryption precision than the past technique.

KEYWORDS: Innovation, Clamorous, Encryption, Algorithm, Framework.

INTRODUCTION

The term digital image refers to processing of a two dimensional picture by a digital computer .In electrical engineering and computer science, image processing is any form of processing for which the input is an image ,such as photographs or video frames, the output can be either image or set of parameters or characteristics of that image. With the rapid development in computer network and in several processes. Normally encryption is a process which uses finite set of instruction called an algorithm to convert original text known as plain text into an encrypted text known as cipher text. Cryptographic algorithms normally require a set of characters called a key to encrypt and decrypt text. Image encryption plays an important role in image hiding.

[*]Lecturer-II, DMI St. John the Baptist University.
[**]Director of Education, DMI Group of Institutions, Africa.
Correspondence E-mail Id: editor@eurekajournals.com

 ISSN: 2581-3609

Due to the advancement in network technology, security threats to images from unauthorized access by users has been increasing. Therefore security of images during transmission among a communication network is very important. Image encryption method presents information which is unreadable in a image. Therefore no hackers or unauthorised users or eaves dropper including server administrators and others have access to the original message or any other type of information through public networks like internet without an image encryption key. Image encryption plays a significant role in information hiding. It is very complicated due to the presence of some internal features like the chaotic properties like the boundedness, intrinsic randomness and sensitivity to initial conditions that meets the demand for image encryption. To gain a consistent method for image encryption, several researches has been done by scientists. Several encryption algorithms are in assortment from defense and intelligences use them in profitable undertakings on a daily basis. An expertise has to be taken into account for simpler and improved encryption techniques and cryptanalysis. Codes have been turned out to be further progressive developing from simple character replacement ciphers to today's algorithm of large pseudo- primes, exponents with large measures of consistency of data security. Chaos has been seen to be involved in various natural and laboratory systems where a significant number of scientific and engineering and technological areas (physics, biology, meteorology, ecology, electronics, computer science and economy). In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the image encryption techniques, and then be transmitted through the internet rapidly. Many different carrier file formats can be used to hide the images or any other files, but digital images are the most popular because of their frequency on the internet. The problem of security of image information transmission and storage draws more attention. Image encryption techniques are very much useful for safe and secured transmission of digital images over communication networks. The image encryption technique is far different from the text encryption and is more complicated. The chaotic some particular laws of evolution and so, they are deterministic in nature. It must be said that chaos happens only in non deterministic non linear systems.

In terms of secure communication, lower dimensional integer chaotic systems are more easily implemented than higher ones. But the major fact is that image encryption security of higher dimensional chaotic systems is better than the lower ones.

The chaotic system consists of mathematical concepts for the purpose of encryption. Obviously chaos give the impression as if there is a nonstop and disorderly looking elongated evolution that fulfils certain mathematical standards. Normally, these type of systems follow encrypted images and their transmission over a communication network. The chaotic systems and their implementation need a enormous explanation with a specific sort of dynamical action. The chaotic systems are impulsive in maintaining the security communication systems. There is a set of features that encapsulate the characteristics perceived in chaotic systems. These are deliberated as the mathematical standards that define chaos. The most appropriate ones are as follows:

DYNAMIC INSTABILITY

This characteristics of the chaotic systems is also mentioned as the butterfly effect. It is the

 ISSN: 2581-3609

property of sensitivity to preliminary state of affairs, where two randomly closed preliminary situations progress with considerably dissimilar and deviating trajectories.

APERIODICITY

The system progresses in an orbit that on no occasion replicates itself, that is the these orbits are never periodic.

TOPOLOGICAL MIXING

The chaotic systems are spontaneously represented as mixing coloured dyes, which explains that the system will progress in time so that any specified section of states is constantly converted or overlaps with any other specified solutions.

DENSE PERIODIC ORBITS

It explains that the chaotic systems follows a dynamics that can diligently approach every potential asymptotic state in random.

SELF SIMILARITY

The progression of the system, in time and space, demonstrates the similar presence at dissimilar scale of abstraction in the chaotic systems.

ERGODICITY

The arithmetic capacity of the variables that are used in the integer related chaotic systems give related outcomes no matter if they are executed over time or space. Other way around, the dynamics indicates alike statistics when measured over space or time in chaotic systems.

These distinctive features create the systems to appear as auto repetitive at dissimilar scale of observation.

RELATED WORK

The chaos based encryption and cryptosystems have been widely used and investigated in recent years to provide real time encryption and transmission. The Chen chaotic systems is proposed as a pseudorandom sequence generator for inter based or fractional chaotic measures for efficient and secured encryption and cryptanalysis. A new algorithm is generated to solve the problem of non conformance to uniform distribution of the sequence generated by the Chen chaotic systems.

Statistical analysis and security analysis show that it has good pseudorandom characteristics and is highly capable of withstanding attacks. Pseudorandom binary sequences have a significant role in numerous applications, amongst other control coding, speed spectrum communication and cryptanalysis. Most methods for generating pseudorandom number sequences are based on mid square method, the linear congruence methods, the linear and nonlinear feedback shift register etc.

Based on complex Chen systems and complex Lorent system a novel, colour image encryption algorithm is proposed. Large chaotic ranges and more complex behaviour of complex chaotic systems when compared to real chaotic systems should additionally enhance the security and large key space of colour image encryption.

The encryption algorithm consists of three processes in the permutation process, the pixels of plin image are scrambled via two dimensional and one dimensional permutation processes among RGB channels of the image individually. In the diffusion process Xor operation is used to conceal pixel information. The proposed algorithm has large key space, high security and robustness against potential attacks and wonderful immunity to noise interferences during the image processing. The disadvantages of the system is that a small key space is provided for the cryptosystems which may be difficult for the cryptanalysis process.

 ISSN: 2581-3609

The chen subsystem has following basic dynamical properties:

According to the definition of Lyapunov exponents, when selecting parameters a = 35, b = 3, c = 28 with initial values $x(0)$ = 3, $y(0)$ = 1, and $z(0)$ = 5, we could get the Lyapunovexponents of subsystem (1) as: $L1$ = 2.0074, $L2$ = 0 and$L3$ = −19.2303. The subsystem (1) displays chaotic behavior since one of the Lyapunov exponents is positive [24]. For the case of choosing the same parameters and initial conditions, chaotic attractors of the subsystem (1) in different phase planes

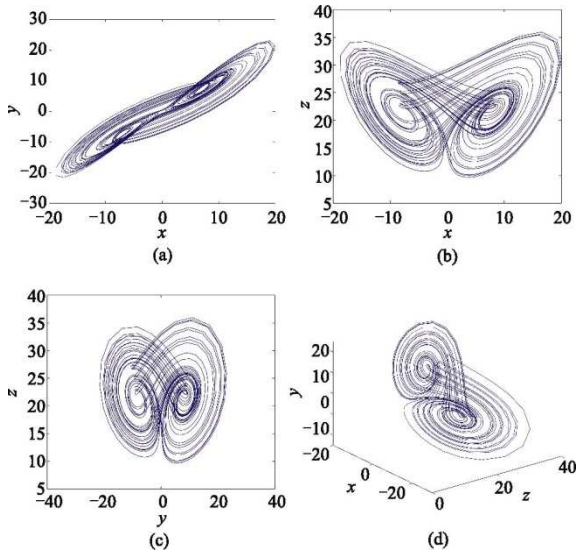


Figure 1.Lyapunov Exponents and Bifurcation Diagram

Bifurcation means a change, a splitting apart and a division into two branches. The bifurcation diagram and Lyapunovexponent spectrum for subsystem (1) due to the variation of parameters a and b are investigated in this paper. For subsystem (2) and subsystem (3), those could also be discussed similarly and will be omitted.

From Fig. 2, we could see that when 33< a < 46, subsystem (1) is chaotic.

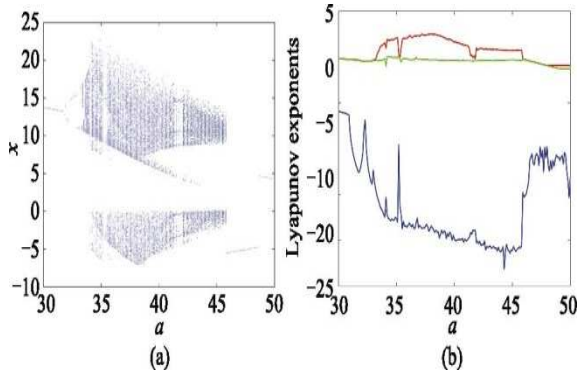


Figure 2.Bifurcation diagram and Lyapunov exponent spectrum with respectto parameter *a*. (a) Bifurcation diagram. (b) Lyapunov exponent spectrum

From Fig. 3, conclusion could be obtained that when 0< b< 4.2, subsystem (1) shows chaotic behavior.

 ISSN: 2581-3609

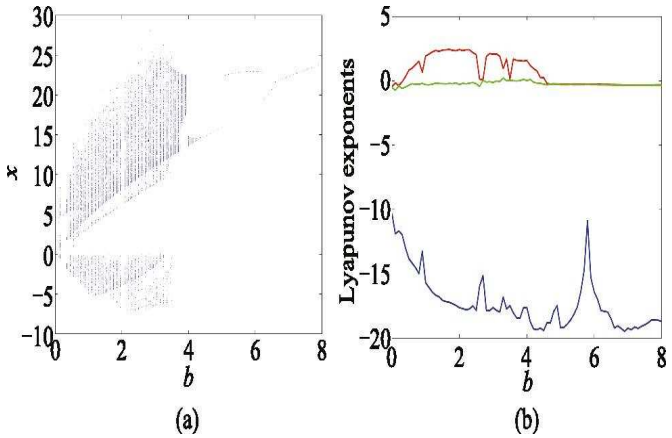


Figure 3.Bifurcation diagram and Lyapunov exponent spectrum with respectto parameter *b*. (a) Bifurcation diagram. (b) Lyapunov exponent spectrum

FRACTAL DIMENSION

Dissipation:

The formula is

so the subsystem (1) $= -a + c - b = -10 < 0$ (5)

is dissipative, converging at exponential rate e_10t. In other words, the initial volume element is V (0) and becomes V (t) = V (0)$e\_^{10t}$ in time t. When $t \rightarrow \infty$, every volume element which contains trajectories of the subsystem (1) shrinks to zero with the rate of exponential convergence.

EQUILIBRIUM POINTS AND STABILITY

The equilibrium points of subsystem (1) could be calculated by making subsystem (1) = 0, we get three equilibrium points of the sub system(1) as

$E1$ = (0, 0, 0)

$E2$ = (7.937, 7.937, 21)

$E3$ = (−7.937, −7.937, 21).

By linearizing the subsystem, we get the result as above.

In the face of those problems, some researchers have made their contribution in last several years, which may sum up four directions. They are introducing the multi-dimension or complex chaotic map combining several chaotic maps designing more complex permutation-diffusion algorithm and adding some traditional encryption methods Liu and Wang proposed a spatial bit-level permutation method based on high-dimension chaotic system. Wang proposed a new chaotic encryption algorithm with the perceptron conception of a neural network. Each of them has its advantages, the drawbacks also exist meanwhile. The key space is not larger enough than multi-dimension. But the condition is different from the proposed algorithm based on combination of two complex chaos systems. Besides, the correlations between each channel are neglected by most algorithms, which is more vulnerable to attacks Wang et al. proposed an algorithm to make three components affect each other. This is a good idea and reducing correlations is also considered to design our algorithm.

Therefore, our proposed scheme in this paper based on complex Chen system and complex Lorenz system may enlarge key space against potential attacks. In addition, we modify the pixels confusion section with the two-dimensional process and add one step process at last, whose main idea is to mix RGB channels using pseudorandom number

 ISSN: 2581-3609

sequences generated by complex chaotic system. The outstanding characteristics is in the multilevel diffusion and large key space. All those combined processes may ensure the security, resist attacks and avoid existing problems discussed above in all directions. Finally, in order to test the stability of our theory, we introduce two noise including Gaussian noise and occlusion to test it.

Pseudo-randomness is the basic property of chaotic system, which is suitable for encryption to cover information. For simplicity and high-level efficiency, one-dimensional chaotic systems, such as logistic map, are widely employed to generate the pseudorandom number sequences. However, their drawbacks, such as small key space, are so obvious that many proposed chaotic cryptosystems have been broken by some cryptanalytic methods. The real part and imaginary part of complex variables from complex chaotic systems double the number of real variables, which increase complex and random. Therefore, complex Chen system and complex Lorenz system are employed to overcome the weakness and enhance the security.

The mentioned critical chaotic system is described by

$$x^{\cdot} = a(y - x)$$

$$y^{\cdot} = -xz + cy$$

$$z^{\cdot} = xy - bz$$

which has a chaotic attractor as shown when a = 36, b = 3, c = 20. To further investigate the joint function of this new chaotic attractor, a constant control term is added to the third equation:

$$x^{\cdot} = a(y - x)$$

$$y^{\cdot} = -xz + cy$$

$$z^{\cdot} = xy - bz + m.$$

When m = 40, it has a similar topological structure to the Lorenz attractor, as shown while when m = −300, it has similar topological structure to the Chen attractor. Linearizing the controlled system (2) about the equilibrium S0 provides an eigenvalue λ1 = −b along with the following characteristic equation:

$$f(\lambda) = \lambda 2 + (a - c)\lambda + a(m - bc)\, b = 0$$

When m < bc, the two eigenvalues satisfy λ2 > 0 > λ3, so the equilibrium S0 is a saddle point in three-dimension; when m > bc and a bc and a>c, the equilibrium S0 becomes a sink. Next, linearizing the system about the other equilibria yields the following characteristic equation:

$$f(\lambda) = \lambda 3+(a+b-c)\lambda 2+(ab-m)\lambda+2a(bc-m)=0 .$$

Obviously, the two equilibria S± have the same stability. The Routh–Hurwitz conditions lead to the conclusion that the real parts of the roots λ are negative if and only if $a + b - c > 0$, $2a(bc - m) > 0$ and $(a + b - c)(ab - m) - 2a(bc - m) > 0$. Therefore: (i) if a+c>b, then when m > (ab(3c−a−b)/(a+ c − b)), the equilibria S± are sinks; (ii) if a+c< (ab(3c−a−b)/(a+ c − b)), the equilibria S± are sinks. In the following, assume that a>c. For the equilibria S±, one has $bc - m > 0$ and $ab - m > bc - m > 0$.

Note that the coefficients of the cubic polynomial (4) are all positive. Therefore, $f(\lambda) > 0$ for all $\lambda > 0$. Consequently, there is instability ($Re(\lambda) > 0$) only if there are two complex conjugate zeros of f. Now, it is clear that when m = bc, the three zeros are λ = 0, −(a−c), −b, and therefore the system has linear stability or marginal stability. The first zero gives $\lambda \sim -(2a(bc - m)/(ab - m))$, as m ↑ bc, so stability is lost in the limit as m approaches bc from below. As m decreases from bc, instability can set in only when $Re(\lambda) = 0$,

 ISSN: 2581-3609

COMPLEX LORENZ SYSTEM

The complex Lorenz system is described as a system of ordinary differential equations first studied by Edward Lorenz. It is notable for having chaotic solutions for certain parameter values and initial conditions. In particular, the **Lorenz attractor** is a set of chaotic solutions of the Lorenz system which, when plotted, resemble a butterfly or figure eight.

The model is a system of three ordinary differential equations now known as the Lorenz equations:

The equations relate the properties of a two-dimensional fluid layer uniformly warmed from below and cooled from above. In particular, the equations describe the rate of change of three quantities with respect to time It is proportional to the Prandtl number, Rayleigh number, and certain physical dimensions of the layer itself.

The Lorenz equations also arise in simplified models for lasers, dynamos, thermosyphons, brushless DC motors, complex electric circuits, chemical reactions and forward osmosis.

From a technical standpoint, the Lorenz system is nonlinear, non-periodic, three-dimensional and deterministic. The Lorenz equations have been the subject of hundreds of research articles, and at least one book-length.

The Lorenz equations are derived from the Oberbeck-Boussinesq approximation to the equations describing fluid circulation in a shallow layer of fluid, heated uniformly from below and cooled uniformly from above. This fluid circulation is known as Rayleigh-Bénard convection. The fluid is assumed to circulate in two dimensions (vertical and horizontal) with periodic rectangular boundary conditions.

The partial differential equations modelling the system's function and temperature are subjected to a spectral Galerkin approximation: the hydrodynamic fields are expanded in Fourier series, which are then severely truncated to a single term for the stream function and two terms for the temperature. This reduces the model equations to a set of three coupled, nonlinear ordinary differential equations. A detailed derivation may be found, for example, in nonlinear dynamics texts. The Lorenz system is a reduced version of a larger system studied earlier by Barry Saltzman.

PROPOSED SYSTEM

Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, the density of the set of all periodic points and topological transitivity, etc. Most properties are related to some requirements such as mixing and diffusion in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications.

The encryption algorithm proposed in this paper is based on a permutation-diffusion architecture. In the diffusion stage, the fractional-order Chen chaotic system is employed to generate the key stream for diffusion, and the pixel values are modified sequentially to confuse the relationship between the cipher-image and the plain-image. In some existing chaos-based image ciphers, the key stream used in the diffusion process is solely determined by the key.

The same key stream is applied to encrypt different plain-images if the key remains unchanged. An opponent may derive the key stream by the plain-text attack, i.e., by ciphering some special plain-text sequences and then comparing them with the corresponding cipher-text sequences. In order to make the cryptosystem secure against a differential attack, the modification made to a particular pixel depends not only on the

 ISSN: 2581-3609

corresponding key stream element, but also on the accumulated effect of all previous pixel values.

The objective of this paper is to propose a new switching fractional order chaotic system for image encryption. XOR operation is used in the image encryption. For security analysis histogram analysis is used. Histogram reflects the basic statistical characteristics of images. In the encryption scheme, key space should be sufficiently large to resist brute-force attack. The security analyses show that the encryption scheme has a larger key space and higher sensitivity to key parameters. Additionally, it also has stronger randomness and faster speed in encryption process.

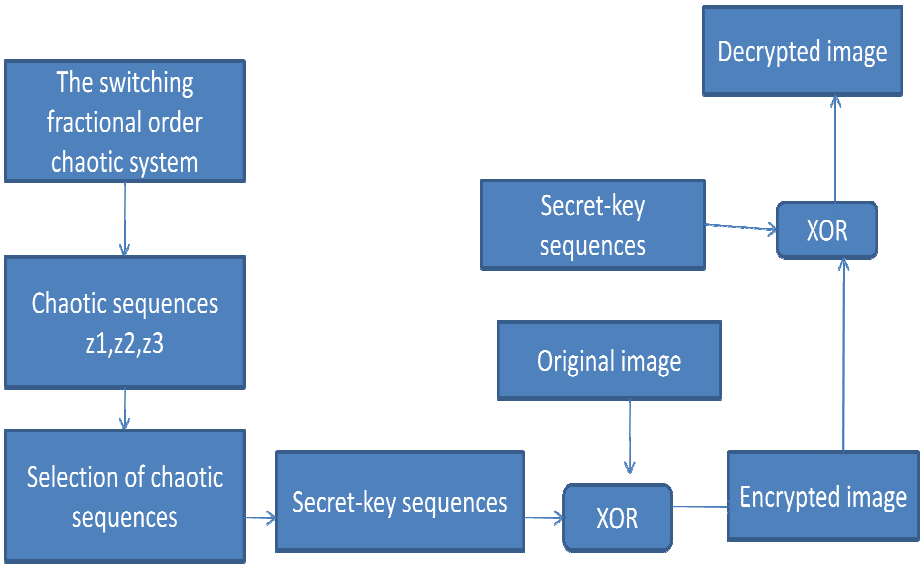
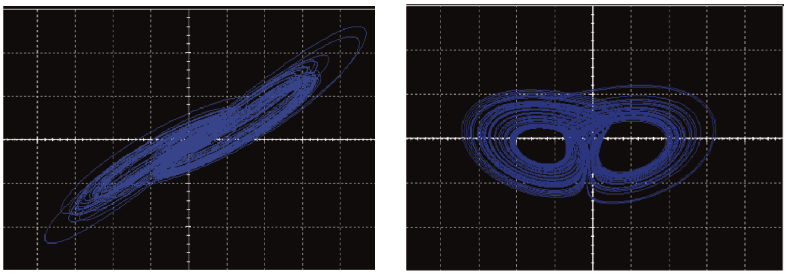


Figure 4.Block diagram

THE SWITCHING FRACTIONAL ORDER SYSTEM

To gain a consistent method for encryption has been always in need even all over the past. Several encryption applications are in an assortment from defense and intelligences utilize in profitable undertakings on daily basis. An expertise has enhanced to take into account simpler and improved encryption and transmission, hence it has also permitted the development in interception and cryptanalysis. Codes have been turn out to be further progressive, developing from simple character replacement ciphers to today's algorithm of large pseudo-primes, exponents, and particular consistency. In any case the idea has stayed basic; it is anticipated to have the capacity to send data starting with one point then onto the next without any one having the capacity to comprehend it in the mid. The appearance of the web has made security of information and assurance of protection a significant reason for concern toward anybody. The profoundly eccentric and irregular look nature of chaotic signals is the most tempting feature of deterministic chaotic system that may prompt to as novel applications. With the quick advancement of the computer innovation and data processing technology, the issue of data security is constantly more imperative.

 ISSN: 2581-3609



(a) (b)

Figure 5.A &b simulations of chaotic systems

SELECTION OF CHAOTIC SEQUENCES

In this paper, XOR operation is used in the image encryption and it has the following rule:

m XOR $f(z)$ XOR $f(z) = m$ (13)

where, m is pixel value of the image,

$f(z)$ is key sequence generated by the switching fractional order chaotic system and $f(z)$ has the following rules:

$f(z) = z_1$, $0 \le m < 85$

z_2, $85 \le m < 170$

z_3, $170 \le m \le 255$

The encrypted image is obtained performing logic XOR operation between m and $f(z)$. Similarly, decrypted image could be obtained by performing the same operation between encrypted image and $f(z)$. Therefore, process of encryption and decryption could be realized by using the same secret-key sequence.

CONCLUSION AND FUTURE WORK

In this paper, uses a new switching fractional order chaotic system, which is composed of three fractional order chaotic subsystems. With regard to the switching fractional order chaotic system, chaotic attractors are shown firstly, and then dynamical properties are discussed, switching among the three subsystems is allowed by controlling switch $k1$ and $k2$, the results of circuit simulations and numerical simulations are basically the same. Therefore, the proposed switching fractional order chaotic system is valid. At last, I apply it to image encryption by using XOR operation. The security analyses show that the encryption scheme has a larger key space and higher sensitivity to key parameters. Additionally, it also has stronger randomness and faster speed in encryption process. In existing a key is used for image encryption. In future image is used for encryption.

REFERENCES

[1]. L. Y. Wang, H. J. Song, and P. Liu, “A novel hybrid color image encryption algorithm using two complex chaotic systems,” *Opt. Lasers Eng.*, vol. 77, pp. 118*j*125, Feb. 2016.

[2]. X. Y. Wang, L. Teng, and X. Qin, “A novel colour image encryption algorithm based on chaos,” *Signal Process.*, vol. 92, no. 4, pp. 1101*j*1108, Apr. 2012.

[3]. X. Y. Wang and M. J. Wang, “A hyperchaos generated from Lorenz system,” *Phys. A: Statist. Mech. Appl.*, vol. 387, no. 14, pp. 3751*j*3758, Jun. 2008.

[4]. Y. G. Zhang, J. Y. Yang, K. C. Wang, Z. P. Wang, and Y. D. Wang, “Improved wind prediction based on the Lorenz system,” *Renew. Energy*, vol. 81, pp. 219*j*226, Sep. 2015.

[5]. X. X. Liao, H. G. Luo, G. Zhang, J. G. Jian, X. J. Zong, and B. J. Xu, “New results on global synchronization of Chua’s circuit,” *Acta Automat. Sin.*, vol. 31, no. 2, pp. 320*j*326, Mar. 2005.

 ISSN: 2581-3609

[6]. H. P. Hu, L. F. Liu, and N. D. Ding, “Pseudorandom sequence generator based on the Chen chaotic system,” *Comp. Phys. Commun.*, vol. 184, no. 3, pp. 765*¡*768, Mar. 2013.

[7]. N. Smaoui, A. Karouma, and M. Zribi, “Secure communications based on the synchronization of the hyperchaotic Chen and the unified chaotic systems,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 8, pp. 3279*¡*3293, Aug. 2011.

[8]. Y. J. Liu and G. P. Pang, “The basin of attraction of the Liu system,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 4, pp. 2065*¡*2071, Apr. 2011.

[9]. [9] Y. K. Li, “The stability of hybrid Liu chaotic system with a sort of oscillating parameters under impulsive control,” *Phys. Proc.*, vol. 24, pp. 490*¡*495, Dec. 2012.

[10]. A. E. Matouk, “Dynamical analysis, feedback control and synchronization of Liu dynamical system,” *Nonlin. Anal.: Theory Meth. Appl.*, vol. 69, no. 10, pp. 3213*¡*3224, Nov. 2008.

[11]. A. Algaba, F. Fern´and ez-S´anchez, M. Merino, and A. J. Rodr´ıguez-Luis, “Centers on center manifolds in the Lorenz, Chen and L¨u systems,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 4, pp. 772*¡*775, Apr. 2014.

[12]. G. A. Leonov and N. V. Kuznetsov, “On differences and similarities in the analysis of Lorenz, Chen, and Lu systems,” *Appl. Math. Comput.*, vol. 256, pp. 334*¡*343, Apr. 2015.

[13]. A. Algaba, F. Fern´andez-S´anchez, M. Merino, and A. J. Rodr´ıguez-Luis, “The L¨u system is a particular case of the Lorenz system,” *Phys. Lett. A*, vol. 377, no. 39, pp. 2771*¡*2776, Nov. 2013.

[14]. J. W. Wang, X. H. Xiong, and Y. B. Zhang, “Extending synchronization scheme to chaotic fractional-order Chen systems,” *Phys. A: Statist. Mech. Appl.*, vol. 370, no. 2, pp. 279*¡*285, Oct. 2006.

[15]. A. S. Hegazi and A. E. Matouk, “Dynamical behaviors and synchronization in the fractional order hyperchaotic Chen system,” *Appl. Math. Lett.*, vol. 24, no. 11, pp. 1938*¡*1944, Nov. 2011.

 ISSN: 2581-3609